HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/099,779	03/14/2002	Todd Weston Arnold	AUS920010984US1	4841

40412 7590 09/19/2005

IBM CORPORATION- AUSTIN (JVL)
C/O VAN LEEUWEN & VAN LEEUWEN
PO BOX 90609
AUSTIN, TX 78709-0609

EXAMINER
WILLIAMS, JEFFERY L

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

15

Office Action Summary	**Application No.** 10/099,779	**Applicant(s)** ARNOLD ET AL.	
	Examiner Jeffery Williams	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1 – 8 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. These claims are non-statutory as all of the claimed features can be implemented in software alone. Thus, these claims are rejected as not being tangible.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Al-Salqan, "Method and Apparatus for Encoding Keys", U.S. Patent, 6,549,626 in view of Hosokawa, "Internet Broadcast Billing System", U.S. Patent Publication, 2001/0023416 A1.

Regarding claim 1, Al-Salqan discloses:

receiving a first password corresponding a software application (Al-Salqan, col. 2, lines 12-28, 49-63); *generating a first mask value based on the first password* (Al-Salqan, col. 4, lines 29-46); *combining the first mask value with a first encryption key* (Al-Salqan, col. 4, lines 49-52);

receiving a second password corresponding to the software application (Al-Salqan, col. 2, lines 12-28, 49-63; fig. 3); *generating a second mask value based on the second password* (Al-Salqan, col. 4, lines 29-46; fig. 3);

separating a recovered encryption key from the tied key using the second mask value (Al-Salqan, col. 7, lines 45-49; fig. 3),

encrypting data using the recovered generated key (Al-Salqan, Abstract, lines 1-3; col. 7, lines 37-49; col. 3, lines 52-56). Al-Salqan discloses the encryption of symmetric encryption keys. When an encryption key becomes lost, an authorized user of the key may recover the key for use. Al-Salqan discloses that such symmetric encryption keys are used to encrypt and decrypt data.

Al-Salqan discloses a system designed to ensure the secrecy of a data encryption key, such as a symmetric key. Secrecy is accomplished by encrypting the data encryption key. However, though Al-Salqan discloses enabling the secrecy of a symmetric data encryption key, it does not disclose the enabling of the authenticity of the key. Thus, Al-Salqan does not disclose wherein the first “encryption key” *is derived from a generated key and a known value the combining resulting a tied key* or that the recovered "encryption key" includes *a recovered generated key and a recovered known value*.

Hosokawa discloses a method for the verification of the authenticity of a data-encryption key, the method being performed "as a security measure" (Hosokawa, par 37). This "security measure" of ensuring authenticity is additional to the security measure of ensuring secrecy - encrypting the data encryption key. The method comprises the creation of a "tied key", or an "encryption key" derived from a generated key and a known value (Hosokawa, par. 32, lines 8-12; par. 33, lines 1-5; par. 37, lines 11-13; par. 44, lines 11-18). Hosokawa attaches a "known value", a digital signature, to generated key, and thereby creates a "tied key". After the "tied key" is decrypted, the attached digital signature is compared to an authentic digital signature so as to verify the authenticity of the generated key. If authentic, the generated key is used for encrypting data. Thus, Hosokawa discloses a method usable to verify the authenticity of an encryption key, the method ensuring a measure of security.

It would have been obvious to one of ordinary skill in the art to combine the method of Hosokawa with the system of Al-Salqan. This would have been obvious because one of ordinary skill in the art would have been motivated to enhance the security of the system of Al-Salqan, by not only enabling the secrecy of the data encryption key, but also the authentication of the data encryption key. Thus, a more secure system is provided.

Regarding claim 2, the combination of Al-Salqan and Hosokawa disclose:

encrypting the tied key using second encryption key, the encrypting resulting a first encrypted tied key; returning the first encrypted tied key to the software application (Al-Salqan, col. 2, lines 54-64; col. 3, lines 16-46; col. 7, lines 1-9).

Regarding claim 3, the combination of Al-Salqan and Hosokawa disclose:

receiving a second encrypted tied key; and combining the second encrypted tied key with second encryption key, the combining resulting in a recovered tied key (Al-Salqan, col. 7, lines 37-49; Hosokawa, par. 32, lines 9,10).

Regarding claim 4, the combination of Al-Salqan and Hosokawa disclose:

determining whether a matched encryption tied key is available corresponding to the second encryption key; and sending the matched encryption tied key security module response to the determination (Al-Salqan, col. 2, lines 50-57; col. 4, lines 47-65; fig. 5).

Regarding claim 5, the combination of Al-Salqan and Hosokawa disclose:

determining whether a matched encrypted tied key available corresponding to the second encryption key; and sending the first password to a security module response to the determination (Al-Salqan, col. 2, lines 50-57; col. 4, lines 47-65; fig. 5).

Regarding claim 6, the combination of Al-Salqan and Hosokawa disclose:

determining whether the recovered known value is correct; and processing a data file based on the determination (Hosokawa, col. 2, pars. 32, 33; Al-Salqan, Abstract, lines 1-3; col. 7, lines 37-49; col. 3, lines 52-56).

Regarding claim 7, the combination of Al-Salqan and Hosokawa disclose:

wherein the processing is selected from the group consisting of encrypting the data file using the recovered generated key and decrypting the data file using the recovered generated key (Al-Salqan, Abstract, lines 1-3; col. 7, lines 37-49; col. 3, lines 52-56).

Regarding claims 8 – 20, they are the system means and computer program product claims implementing the method of claims 1 – 7, and are rejected for the same reasons. Further, regarding claim 8 specifically, it is rejected because the combination of Al-Salqan and Hosokawa disclose:

one or more processors; a memory accessible by the processors; one or more nonvolatile storage devices accessible by the processors; a hardware security module accessible by the processors; a data security tool for securing data using the hardware security module (Al-Salqan, figs. 1, 2; col. 3, lines 16-45).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Al-Salqan, “Methods and Apparatus for Recovering Keys”, U.S. Patent 6,160,891.

A shortened statutory period for reply is set to expire **3** months (not less than 90 days) from the mailing date of this communication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
Assistant Examiner
Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER